Abstract

RC4 is a stream cipher cryptographic algorithm commonly used in security protocols. The algorithm consists of three main steps, initialization array, KSA, and PRGA, to generate a keystream to be used in the process of encryption and decryption. Process on the RC4 encryption and decryption implemented by XOR operation between the keystream and plaintext. RC4 can be implemented with a variable key length and byte-oriented operations.

RC4 encryption method has several drawbacks. One of the well-known weakness of RC4 encryption is Bit Flipping Attack(BFA),which the attacker can have the access to know a sample or a whole plaintext from ciphertext without knowing the encrytion key. At this final project proposed modification to handle that problem CRC Bit Flipping Attack. The modification is done by giving CRC-32 bit is applied on the plaintext before encryption process and after encryption process the CRC values are recalculated.

The results of tests performed on the RC4 algorithm, the addition of the CRC calculation on the plaintext prior to encryption process, managed succesfully to improve data security from Bit Flipping Attack. The quality of the generated RC4 with CRC cryptography in this system is affected by the value of the avalanche effect and time of execution process. Thequality of plaintext avalanche effect for the same conditions with different key value of the avalanche effect RC4 modification of CRC as well as the avalanche effect resulting from RC4 modification of CRC key in the same conditions with different plaintext. On the RC4 algorithm ciphertext message length is shorter than 4 bytes CRC so that the modified RC4 encryption / decryption's time execution is faster than RC4 modification of CRC.

Key words: RC4, encryption, decryption, Bit Flipping Attack, CRC.